REMARKS

Claims 1-20 remain pending in the application, with claims 1-14 withdrawn from consideration because of a restriction requirement.

Restriction

The Applicants reiterate the election of claims 15-20 in response to a restriction requirement issue by the Examiner, with traverse.

Claims 15, 16, 18 and 19 over DiFrancisco in view of KIV Family

In the Office Action, claims 15, 16, 18 and 19 were rejected under 35 U.S.C. §103(a) as allegedly being obvious over *Global Broadcast Service (GBS) End-to-End Services: Protocols and Encapsulation* by Michael DiFrancisco et al. ("DiFrancisco") in view of *KIV-7 Family* ("KIV Family"). The Applicants respectfully traverse the rejection.

Claims 15, 16, 18 and 19 recite routing network data from a plurality of sources by a red side router, the plurality of sources comprising telephony devices and computing devices; and routing IP encapsulated, bulk encrypted data, through a black side router, from an output port of a portable, deployable communication system over a **public Internet**.

DiFrancisco discloses eight different end-to-end data services to end users based on encapsulation, the data services being passed from a Transmit Suite to a Receive Suite (see Abstract). However, DiFrancisco fails to disclose, teach or suggest use of two **different types** of routers, much less disclose routing network data from a plurality of sources by a red side router, the plurality of sources comprising telephony devices and computing devices; and routing IP encapsulated, bulk encrypted data, through a black side router, from an output port of a portable, deployable communication system over a **public Internet**, as recited by claims 15, 16, 18 and 19.

The Office Action acknowledged that DiFrancisco fails to teach KIV type encryption devices (Office Action, page 4). The Office Action relied on KIV Family to allegedly make up for the deficiencies in DiFrancisco. The Applicants respectfully disagree.

KIV Family appears to describe the KIV-7 family of embeddable KG-84 communications security (COMSEC) modules that are lightweight, compact, commercial off-the-shelf (COTS) cryptographic devices that provide protection for digital and voice communications (see first paragraph). The miniaturization of the KIV-7 family units make them suitable for space and load constrained environments such as, e.g., aboard submarines or vehicle mount (see KIV Family first paragraph).

Thus, KIV Family discloses a family of encryption devices. However, KIV Family, like DiFrancisco, fails to disclose, teach or suggest disclose, teach or suggest use of two **different types** of routers for communicating IP encapsulated, bulk encrypted data, much less disclose routing network data from a plurality of sources by a red side router, the plurality of sources comprising telephony devices and computing devices; and routing IP encapsulated, bulk encrypted data, through a black side router, from an output port of a portable, deployable communication system over a **public Internet**, as recited by claims 15, 16, 18 and 19.

DiFrancisco in view of KIV Family, either alone or in combination, would still fail to disclose, teach or suggest disclose, teach or suggest use of two **different types** of routers for communicating IP encapsulated, bulk encrypted data, much less disclose routing network data from a plurality of sources by a red side router, the plurality of sources comprising telephony devices and computing devices; and routing IP encapsulated, bulk encrypted data, through a black side router, from an output port of a portable, deployable communication system over a **public Internet**, as recited by claims 15, 16, 18 and 19.

A benefit two **different types** of routers, i.e., a black side router and a red side router, the ability to route secret information distinct from non-secret information. In some instances, a user may determine that information that is being communicated is with a remote location is non-secret. The information can therefore be routed separately through a black side router to avoid encryption. Avoiding encryption can significantly increase information throughput, which may be highly desirable under certain non-secret

circumstances. In other instances, a user may determine that information that is being communicated with a remote location is secret and requires routing through a red side router for encryption purposes. The cited prior art fails to disclose, teach or suggest the claimed features having such benefits.

Accordingly, for at least all the above reasons, claims 15, 16, 18 and 19 are patentable over the prior art of record. It is therefore respectfully requested that the rejection be withdrawn.

Claims 17 and 20 over DiFrancisco in view of KIV Family and ViaSat

In the Office Action, claims 17 and 20 were rejected under 35 U.S.C. §103(a) as allegedly being obvious over DiFrancisco in view of KIV Family, and further in view of *KIV-21 ViaSat IP Crypto* ("ViaSat"). The Applicants respectfully traverse the rejection.

The Applicants respectfully suggest that the need to combine THREE references is an indication of the non-obviousness of claims 17 and 20.

Claims 17 and 20 are dependent on claims 15 and 18, and are allowable for at least the same reasons as claims 15 and 18.

Claims 17 and 20 recite routing network data from a plurality of sources by a red side router, the plurality of sources comprising telephony devices and computing devices; and routing IP encapsulated, bulk encrypted data, through a black side router, from an output port of a portable, deployable communication system over a **public Internet**.

The Office Action relied on ViaSat to allegedly make up for the deficiencies in DiFrancisco in view of KIV Family to arrive at the claimed features. The Applicants respectfully disagree.

The Office Action relied on ViaSat to allegedly disclose KIV-21 (Office Action, page 5). However, KIV-21 appears to disclose an in-line network encryption device to provide Type I encryption for network users (see first paragraph). KIV-21, like DiFrancisco and KIV Family, fails to disclose, teach or suggest use of two **different types** of routers for communicating IP encapsulated, bulk encrypted data, much less disclose routing network data from

a plurality of sources by a red side router, the plurality of sources comprising telephony devices and computing devices; and routing IP encapsulated, bulk encrypted data, through a black side router, from an output port of a portable, deployable communication system over a **public Internet**, as recited by claims 17 and 20.

DiFrancisco in view of KIV Family, and further in view of ViaSat, either alone or in combination, fails to disclose, teach or suggest use of two **different types** of routers for communicating IP encapsulated, bulk encrypted data, much less disclose routing network data from a plurality of sources by a red side router, the plurality of sources comprising telephony devices and computing devices; and routing IP encapsulated, bulk encrypted data, through a black side router, from an output port of a portable, deployable communication system over a **public Internet**, as recited by claims 17 and 20.

Accordingly, for at least all the above reasons, claims 17 and 20 are patentable over the prior art of record. It is therefore respectfully requested that the rejection be withdrawn.

Conclusion

All objections and/or rejections having been addressed, it is respectfully submitted that the subject application is in condition for allowance and a Notice to that effect is earnestly solicited.

Respectfully submitted,

William H. Bollman
Reg. No.: 36,457
Tel. (202) 261-1020
Fax. (202) 887-0336

MANELLI DENISON & SELTER PLLC
2000 M Street, N.W. 7th Floor
Washington D.C. 20036-3307
WHB/df